OffSec WEB-200 (OSWA) Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **5 Day**

Foundational Web Application Assessments with Kali Linux and OSWA Certification

Learn the foundations of web application assessments with Foundational Web Application Assessments with Kali Linux (WEB-200). Learners who complete the course and pass the exam will earn the OffSec Web Assessor (OSWA) certification and will demonstrate their ability to leverage web exploitation techniques on modern applications. This course teaches learners how to discover and exploit common web vulnerabilities and how to exfiltrate sensitive data from target web applications. Learners that complete the course will obtain a wide variety of skill sets and competencies for web app assessments.

Prerequisites

All learners should have basic knolwedge of Web Applications, Linux and Networking.

Target Audience

Anyone interested in expanding their understanding of Web Application Attacks, and/or Infra Pentesters looking to broaden their skill sets and Web App expertise. Job roles include: Web Penetration Testers, Pentesters, Web Application Developers, Application Security Analysts, Application Security Architects, and SOC Analysts and other blue team members.

What You Will Learn

Learners will learn how to:

- Enumerate web applications and four common database management systems
- Manually discover and exploit common web application vulnerabilities
- Go beyond alert() and actually exploit other users with cross-site scripting
- Exploit six different templating engines, often leading to RCE

About the Exam

- The OSWA exam voucher is included in the course, and is a proctored exam
- The WEB-200 course and online lab prepares you for the OSWA certification

Training Outline

Introduction to WEB200

Module 1 Secrets of Success with WEB200

- Understand some of the general concepts surrounding application security
- Recognize the unique mindset of a successful application security professional
- Understand the pillars of prerequisite knowledge for application security

OffSec WEB-200 (OSWA) Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **5 Day**

Introduction to Security Concepts

- Understand the CIA triad and what it means
- Understand other key terms and unique traits of this field
- Understand the basic tools available to students

Getting Started WithWEB200

- Understand the basic tools available tostudents
- Understand how to be 'hands-on' with the material
- Understand how to connect to the VPN

Module 2 Tools

Getting Started

- Learn how to edit the /etc/hosts file
- Understand how to test and confirm that our host file changes are working
- Develop a basic understanding of proxies

Burpsuite

- Learn how to leverage Burp Suite's built-in browser
- Understand how to work fluently with the Proxy tab and Intercept functionality
- Understand how to use both Repeater and Intruder

Nmap

- Understand how to execute an Nmap NSE Script
- Learn how to scan a specific port

Wordlists

- Develop an understanding of the wordlistconcept
- Understand how we attempt to select the best wordlist for our scenario
- Learn the basics needed to construct our own wordlist

Gobuster

- Learn about Retrieval Practice
- Understand Spaced Practice

Wfuzz

- Learn how to discover files using Wfuzz
- Discover how to find directories with Wfuzz
- Understand how to discover parameters with Wfuzz
- Learn how to leverage Wfuzz to fuzz parameters
- Develop the skills to fuzz POST data using Wfuzz

Hakrawler

- Learn what a crawling or spidering tool is
- Understand how hakrawler works with https://archive.org The Wayback Machine) to gather its results

Shells

- Learn how to determine specific the web technology of a web application
- Understand how to choose the correct shell (matching the web technology)

Module 3 Cross-Site Scripting Introduction and Discovery

Introduction to the Sandbox

- Understand how to use the custom sandbox

JavaScript Basics for Offensive Uses

- Understand fundamentals of JavaScript
- Read and understand basic JavaScript code
- Use JavaScript APIs to exfiltrate data

Cross-Site Scripting - Discovery

- Understand the different types of XSS
- Exploit reflected server XSS
- Exploit stored server XSS
- Exploit reflected client XSS
- Exploit stored client XSS

Module 4 Cross-Site Scripting Exploitation and Case Study

Cross-Site Scripting - Exploitation

- Cross-Site Scripting - Exploitation
- Case Study: Shopizer Reflected XSS

Case Study: Shopizer Reflected XSS

- Discover an XSS vulnerability in Shopizer
- Create advanced payloads to load external JavaScript resources
- Discover application-specific attack vectors
- Exploit a Shopizer user using application-specific attacks

Module 5 Cross-Origin Attacks Same-Origin Policy

Penetration Testing Reports

- Understand what an origin is
- Understand the Same-Origin Policy and how it interacts with cross-origin requests

SameSite Cookies

- Understand the concept of cross-origin requests
- Understand the SameSite attribute and its three possible settings

Cross-Site Request Forgery CSRF

- Construct an Executive Summary
- Understand how to identify cross-site request forgery vulnerabilities

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Understand how to exploit cross-site request forgery vulnerabilities

Case Study: Apache OFBiz

- Discover a CSRF vulnerability in a real-world web application
- Exploit a CSRF vulnerability to create a new user
- Use JavaScript to chain multiple CSRF requests
- Understand how the SameSite attribute influences different versions of CSRF attacks

Cross-Origin Resource Sharing CORS

- Understand the concept of CORS
- Understand the common headers found on CORS requests
- Understand the common headers found on

CORS responses Exploiting Weak CORS Policies

- Understand how to identify CORS response headers
- Understand how CORS policies that trust arbitrary origins can be exploited
- Understand how CORS policies that implement incomplete allowlists can be exploited

Module 5 Introduction to SQL

SQL Overview

- Understand the basic syntax of SQL
- Understand how to retrieve data from a table

Enumerating MySQL Databases

- Understand how to identify the version of a MySQL database
- Understand how to identify the schemas within a MySQL database
- Understand how to identify the tables within a schema in a MySQL database
- Understand how to identify the column names and data types in a table in a

MySQL database Enumerating Microsoft SQL Server Databases

- Understand how to identify the version of a SQL Server database
- Understand how to identify the current user of a SQL Server database
- Understand how to identify the databases within a SQL Server instance
- Understand how to identify the tables within a database in a SQL Server instance
- Understand how to identify the column names and data types in a table in a SQL Server database

Enumerating PostgreSQL Databases

- Understand how to identify the version of a PostgreSQL database
- Understand how to identify the current user of a PostgreSQL database
- Understand how to identify the schemas within a PostgreSQL database
- Understand how to identify the tables within a schema in a PostgreSQL database
- Understand how to identify the column names and data types in a table in a PostgreSQL database

Enumerating Oracle Databases

- Understand how to identify the version of an Oracle database

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Understand how to identify the current user of an Oracle database
- Understand how to identify other users or schemas in an Oracle database
- Understand how to identify the tables within a schema in an Oracle database
- Understand how to identify the column names and data types in a table in an Oracle database

Module 6 SQL Injection

Introduction to SQL Injection

- Understand the concept of SQL injection
- Understand how the OR operator can modify the results of a SQL query

Testing for SQL Injection

- Understand how to test web applications to identify SQL injection vulnerabilities
- Understand the basics of where injections points may occur in SQL queries
- How to use fuzzing tools to identify SQL injection vulnerabilities

Exploiting SQL Injection

- Understand how to build and use Error-based payloads
- Understand how to build and use Union-based payloads
- Understand how to use Stacked Queries
- Understand how to use SQL injection to read and write filesinjection vulnerabilities
- Understand the basics of remote code execution in Microsoft SQL Server

Database dumping with Automated Tools

- Understand how to use sqlmap to identify SQL injection vulnerabilities
- Understand how to use sqlmap to obtain a basic OS shell
- Understand how to use sqlmap to create a web shell

Case Study: Error-based SQLi in Piwig

- Discover the parameter vulnerable to SQL injection
- Craft an error-based payload to extract information from the database

Module 7 Directory Traversal Attacks

Directory Traversal Overview

- Understand and work with the results of a vulnerability scan with Nessus
- Provide credentials to perform an authenticated vulnerability scan
- Gain a basic understanding of Nessus Plugins

Understanding Suggestive Parameters

- Understand the basics of the Nmap Scripting Engine NSE
- Perform a lightweight Vulnerability Scan with Nmap
- Work with custom NSE scripts

Relative vs. Absolute Pathing

- Understand what a Traversal String is
- Understand basics of Relative Pathing

- Understand basics of Absolute Pathing

Directory Listing

- Understand what a Directory Listing is
- Understand how to analyze a web application's parameter for directory listing
- Understand what successful exploitation of directory listings looks like

Directory Traversal Sandbox

- Understand how to successfully exploit Directory Traversal
- Understand how to implement Wordlists/Payload Lists
- Understand how to fuzz a potentially vulnerable parameter with Wfuzz

Case Study: Home Assistant

- Understand how our case study of Home Assistant would initially be assessed
- Understand how to exploit this real-world case study
- Understand how to find and discover the documentation for a web application

Module 8 XML External Entities

Introduction to XML

- Understand the basic syntax of XML
- Understand the basic concepts of XML Entities

Understanding XML External Entity Processing Vulnerabilities

- Understand the basic concepts of XML External Entity injection

Testing for XXE

- Understand how to test for XXE injection vulnerabilities
- Learn several techniques for exfiltrating data using XXE vulnerabilities

Case Study: Apache OFBiz XXE Vulnerability

- Identify an XXE vulnerability
- Exploit an XXE vulnerability to exfiltrate data
- Use an error-based XXE payload to exfiltrate data
- Use an out-of-band XXE payload to exfiltrate data

Module 9 Server-side Template Injection - Discovery and Exploitation

Templating Engines

- Understand the purpose of templating engines
- Understand the difference between statements and expressions
- Understand the level of logic a templating engine can have and how it impacts security

Twig - Discovery and Exploitation

- Understand the basic syntax of Twig
- Understand how to discover a Twig template in a black box scenario

- Understand how to reach RCE with a Twig Template

Apache Freemarker - Discovery and Exploitation

- Understand the basic syntax of Freemarker
- Understand how to discover a Freemarker template in a black box scenario
- Understand how to reach RCE with a Freemarker Template

Pug - Discovery and Exploitation

- Understand the basic syntax of Pug
- Understand how to discover a Pug template in a black box scenario
- Understand how to reach RCE with a Pug Template

Jinja - Discovery and Exploitation

- Understand the basic syntax of Jinja
- Understand how to discover a Jinja template in a black-box scenario

Mustache and Handlebars - Discovery and Exploitation

- Understand the basic syntax of Mustache and Handlebars
- Understand how to discover a Handlebars template in a black box scenario
- Understand how to read files on remote servers using a Handlebars Template

Halo - Case Study

- Understand the Halo application
- Discover the template injection and the templating engine used on Halo
- Exploit the template injection in the Halo application

Craft CMS with Sprout Forms - Case Study

- Enumerating the target application
- Discovering the template injection and the templating engine used in Craft CMS and the Sprout Form plugin
- Exploiting the template injection in the application

Module 10 Command Injection

Discovery of Command Injection

- Understand common command injection scenarios
- Understand how to discover command injection
- Understand why we execute the id or whoami commands first
- Understand how we chain commands together and why

Dealing with Common Protections

- Understand what we mean by Input

Normalization

- Understand typical means of Input Sanitization and how we can bypass them
- Understand what Blind OS Command Injection is and how we can work with it

Enumeration & Exploitation

- Understand common enumeration techniques for various capabilities
- Understand how to retrieve a shell with Netcat
- Understand how to retrieve a shell with Python
- Understand how to retrieve a shell with PHP
- Understand how to retrieve a shell with Perl
- Understand how to retrieve a shell with NodejS
- Understand how a couple of reverse shell one-liners accomplish what they do in various languages
- Understand how to transfer files using command injection

Case Study - OpenNetAdmin ONA

- Understand how we discover the command injection in Open Net Admin
- Understand how we exploit the command injection in Open Net Admin

Module 11 Server-side Request Forgery

Introduction to SSRF

- Understand the concept of Server-Side Request Forgery
- Understand how SSRF can interact with the loopback interface
- Understand how SSRF can interact with back-end systems
- Understand how SSRF can interact with private IP ranges

Testing for SSRF

- Understand where SSRF vulnerabilities are likely to occur
- Understand how to test for SSRF
- Understand how to verify SSRF vulnerabilities

Exploiting SSRF

- Understand how to exploit SSRF to retrieve data
- Understand limitations of SSRF
- Understand how SSRF can be exploited in cloud environments
- Become familiar with alternative URI schemes and how they can be used with SSRF

Case Study: Group Office

- Discover the SSRF vulnerabilities
- Exploit the SSRF vulnerabilities

Module 12 Insecure Direct Object Referencing

Introduction to IDOR

- Develop an understanding of Static File IDOR findings
- Learn about Database Object Referencing IDBased) IDOR

Exploiting IDOR in the Sandbox

- Understand how to exploit Static File IDOR
- Learn more about exploiting IDBased IDOR

BILGINC IT Academy

info@bilginc.com

bilginc.com

- Discover how to exploit More Complex IDOR

Case Study: OpenEMR

- Learn how to approach IDOR from a Black Box perspective
- Understand how to discover the vulnerability
- Develop our knowledge of OpenEMR IDOR exploitation

Module 13 Assembling the Pieces: Web Application Assessment Breakdown

Web Application Enumeration

- Understand how to perform basic host enumeration
- Learn how to conduct OS detection
- Develop a working knowledge of content discovery

Authentication Bypass

- Discover a directory traversal vulnerability
- Exploit the directory traversal and obtain the application config file
- Access the admin portion of the web application

Remote Code Execution

- Discover a SQL injection vulnerability
- Exploit the SQL injection vulnerability to obtain remote code execution
- Gain shell access to the server

Exams and Assessments

This course includes the OffSec Web Assessor (OSWA) exam voucher as part of the course fee.

- Certification awarded: OffSec Web Assessor (OSWA)

- Exam format: proctored

- Associated course and exam code: WEB-200

Learners who pass the exam will earn the OSWA certification, demonstrating their ability to leverage web exploitation techniques on modern applications.